Remarks

Claims 1, 3, 26, 27, 28, 30, 31 and 32 have been amended. Claim 2 has been canceled. New claim 33 has been added. No new matter is believed to be added. Moreover, since one dependent claim was canceled and one dependent claim was added, no additional claim fee is believed to be required. Support for the amendment to the claims may be found, for example, at page 2, lines 18-25; page 8, line 21 through page 9, line 19; page 12, lines 4-15; page 13, lines 15-24; and page 14, line 12 through page 15, line 13.

35 U.S.C. §103

Claims 1-3, 5, 7-11, 14, 15 and 26-32 stand rejected under 35 U.S.C. §103(a) as being unpatentable over WO 99/56194 to Bartolomeos *et al.* (hereinafter '*Bartolomeos*') in view of U.S. Pat. Pub. No. 2001/055388 to Kaliski, JR. (hereinafter '*Kaliski*'). According to the M.P.E.P. §706.02(j), to establish a *prima facie* case of obviousness, the prior art reference must teach or suggest all the claim limitations. It is the applicants' position that the art does not support the rejections to the claims, *as amended herein*, thus a *prima facie* case of obviousness has not been established. Accordingly, the applicants respectfully request that the above rejections are withdrawn.

Claim 1:

With respect to claim 1, *Bartolomeos* in view of *Kaliski* fails to teach or suggest at least:

> A method of impersonating a client to a plurality of servers, comprising:
> ...obtaining by a middle tier server, a common nonce that is created based at least in part upon a pre-nonce contribution from each of a plurality of back-end servers, wherein the common nonce is generated from an entity other than the client that the middle tier server is to impersonate or the plurality of back-end servers that the middle tier server is to interact with on behalf of the client...

In *Bartolomeos*, two arrangements are disclosed for a client to authenticate to more than one server in a distributed network. In a first arrangement, a client transmits an access request to a first server. In response thereto, the first server requests authentication data, such as a password and corresponding user identification from the

client. If the client is authenticated, the first server responds to the client by providing the identification of other servers. The *client* then transmits authentication data to each of the other servers and authenticates directly and independently with each server[1]. Each server that the client authenticates with stores a cookie of the client's computer to record state information. Thereafter, the client may directly access a corresponding server by sending a message to the selected server that includes that server's cookie information that had been previously communicated directly to the client.

In the only other disclosed arrangement, the client authenticates to a first server. The first server then forwards the authentication data to other servers. However, the other servers each independently authenticate the client based upon their locally stored authentication data and communicate a cookie containing state *data to the client*. Again, Thereafter, the client may directly access a corresponding server by sending a message to the selected server that includes that server's cookie information that had been previously communicated directly to the client[2].

Kaliski relates to recovering private data, such as a private key, into a stateless client terminal, such as a public terminal, which cannot or does not typically store any data for the user. Essentially, a recovery client interacts with a plurality of "secret holding servers" to recover and regenerate strong secret data. After the strong data is regenerated, a verification process is performed, in which recovery servers each send a nonce to the client. The client may create a message that includes the received nonces, sign the created message and communicate that message back to corresponding verification servers[3].

Bartolomeos, Kaliski and the combination thereof fails to teach or suggest obtaining by a middle tier server, a common nonce that is created based at least in part upon a pre-nonce contribution from each of a plurality of back-end servers, wherein the common nonce is generated from an entity other than the client that the middle tier server

[1] See for example, *Bartolomeos*, page 10, starting at line 17.
[2] See for example, *Bartolomeos*, page 15, starting at line 1.
[3] See for example, *Kaliski*, paragraph 85.

is to impersonate or the plurality of back-end servers that the middle tier server is to interact with on behalf of the client, as recited in claim 1, *as amended herein*.

Moreover, both *Bartolomeos* and *Kaliski* completely fail to even teach a middle-tier server. For example, in *Kaliski*, the client interacts directly with a plurality of peer level secret holding servers. There is no teaching or suggestion of a middle tier server. Additionally, despite the observation by the Examiner that the client in *Kaliski* may create and sign a message the includes a plurality of nonces, there is no teaching or suggestion that a middle-tier server or any other device obtains a common nonce where the common nonce is generated from an entity other than the client that the middle tier server is to impersonate or the plurality of back-end servers that the middle tier server is to interact with on behalf of the client, as recited in claim 1, *as amended herein.*

In *Bartolomeos*, there is no teaching or suggestion of a middle-tier server or any other device for that matter, that obtains a common nonce that is generated from an entity other than the client that the middle tier server is to impersonate or the plurality of back-end servers that the middle tier server is to interact with on behalf of the client, as recited in claim 1, *as amended herein*. In this regard, it is noted that in one disclosed embodiment, a first server forwards client data to other servers. However, this neither teaches nor suggests a middle-tier server as recited in claim 1. For example, in *Bartolomeos*, the first server is not impersonating the client to the other servers. Rather, the first server is passing along information so that each other server can independently and directly authenticate the client[4]. Moreover, in *Bartolomeos,* whenever the client wishes to transact with a server, it does so directly with the corresponding server by supplying its cookie containing the corresponding state data.

Even the combination of references fails to teach or suggest that recited in claim 1, *as amended herein*. For example, taking for sake of argument, the broad interpretation of *Kaliski* that a client can sign a message containing a plurality of nonces and the broad teaching in *Bartolomeos,* that a first server can pass user authentication data to other

[4] See for example, *Bartolomeos*, page 14, lines 1-13.

servers, this still fails to teach or suggest the claimed invention because the references, whether alone or in combination, fail to teach or suggest that a server obtains a common nonce or any other authentication/verification information that is generated from an entity *other than* the client that the middle tier server is to impersonate or the plurality of back-end servers that the middle tier server is to interact with on behalf of the client. In *Bartolomeos,* client authentication data is communicated either directly from the client to each server, or the client information is forwarded from a first server to another. Regardless, all authentication data is generated by the client. In *Kaliski,* the signed message is created by the client[5].

With respect to claim 1, *Bartolomeos* in view of *Kaliski* further fails to teach or suggest at least:

> … receiving by the middle tier server, a request from the client for a transaction with at least one of the plurality of back-end servers …
>
> …providing the common nonce from the middle tier server to the client (wherein the common nonce is generated from an entity other than the client that the middle tier server is to impersonate or the plurality of back-end servers that the middle tier server is to interact with on behalf of the client)
>
> … receiving the common nonce signed by the client with the client's digital signature at the middle-tier server…

As noted above, *Kaliski* relates to recovery of strong secret data from a plurality of servers. *Kaliski* is completely silent with regard to, and fails to teach or suggest a middle tier server and further fails to teach or suggest receiving a request from a client at a middle tier server for a transaction with a back-end server, as recited in claim 1, *as amended herein.* Still further, *Kaliski* fails to teach or suggest providing a common nonce or any other information for that matter, to a client for signature in response to the client communicating a request to a middle tier server for a transaction with at least one of a plurality of back-end servers.

Moreover, as noted in greater detail herein, *Bartolomeos* also fails to teach or suggest a middle-tier server receiving a request from the client for a transaction with at

[5] See for example, *Kaliski,* paragraph 85.

least one of the plurality of back-end servers. In this regard, *Bartolomeos* arguably teaches away from the use of a middle tier server to impersonate a client to a back-end server. This can be seen because in *Bartolomeos,* each of a plurality of servers deposits a cookie on the client computer so that the client can communicate directly with the server by including its cookie as state data to obtain information directly[6]. This is true regardless of whether the servers get authentication directly from the client or from another server. Still further, *Bartolomeos* fails to teach or suggest providing a common nonce or any other information for that matter, to a client for signature in response to the client communicating a request to a middle tier server for a transaction with at least one of a plurality of back-end servers.

Even when the references are combined, there is no teaching or suggestion of providing a common nonce or any other information for that matter, to a client for signature in response to the client communicating a request to a middle tier server for a transaction with at least one of a plurality of back-end servers. As noted in greater detail above, both *Bartolomeos* and *Kaliski* disclose that all client requests for information (at least after authentication) are directed to the corresponding server that provides the information as described more fully herein.

With respect to claim 1, *Bartolomeos* in view of *Kaliski* still further fails to teach or suggest at least:

> …impersonating the client by the middle tier server interacting with a selected one of the plurality of back-end servers for implementation of the client request on behalf of the client by providing the signed common nonce and the client request from the middle tier server to at least one of the plurality of back-end servers so as to authenticate the client to the plurality of servers for implementation of the client request on behalf of the client…

As noted in greater detail herein, the concept of client impersonation is neither taught nor suggested by either reference. Moreover, *Bartolomeos* arguably teaches away from this as each server communicates a cookie to the client so that the client can directly access each server. Further, there is no teaching or suggestion alone or in the

[6] See for example, *Bartolomeos,* page 12, lines 20-25.

combination of *Bartolomeos* and *Kaliski,* that a middle-server or any server for that matter, impersonates a client by providing a signed common nonce and the client request from the middle tier server to at least one of the plurality of back-end servers so as to authenticate the client to the plurality of servers for implementation of the client request on behalf of the client, as recited in claim 1, *as amended herein.*

In support of the rejection, the Examiner argues that *Bartolomeos* teaches a method for a middle tier server to impersonate a client to a plurality of servers[7]. Moreover, the Examiner is relying upon *Barolomeos* for the teaching of a single server that provides the request for authentication data to the client for a plurality of servers. The Examiner further argues that *Kaliski* is being relied upon for the teaching of the client signing a message that includes a plurality of nonces, where each nonce is provided from a different server. The Examiner thus concludes that it would be obvious to one skilled in the art to combine *Barolomeos* with *Kaliski* to collect nonces at a single server, and then transmit a single authentication request to the client[8]. The applicants respectfully traverse this interpretation of the references and their application to claim 1, *as amended herein.*

In this regard, the applicants assert that when claim 1, *as amended herein,* is read *as a whole*[9]*, Bartolomeos, Kaliski* and the combination thereof fails to teach or suggest that which is claimed. Rather, in both cited references, the client deals directly with each of a plurality of servers. For example, in both *Bartolomeos* and *Kaliski*, the servers are peers within a distributed computing environment. Moreover, there is no teaching or suggestion that any server impersonates the client to another server. Merely passing authentication information from one server to another (which *Bartolomeos* admits is not even a workable solution in current HTTP environments[10]) is not impersonation. Thus, the references, alone or in combination fail to teach or suggest providing a signed common nonce and a client request from a middle tier server to at least one back-end

[7] See the Office action mailed November 09, 2007, page 5.
[8] See the Office action mailed November 09, 2007, pages 2-3.
[9] M.P.E.P. §2143; §2143.01; §706.02(j); 35 U.S.C. §103.
[10] See for example, *Bartolomeos,* page 14, lines 7-13.

server so as to authenticate the client to the back-end server for implementation of the client request on behalf of the client.

Even considering *arguendo* that *Kaliski* teaches the broad concept of a client that signs a message containing a plurality of nonces, there is no teaching or suggestion that such a message is obtained by a middle tier server and is generated from an entity other than the client that the middle tier server is to impersonate or the plurality of back-end servers that the middle tier server is to interact with on behalf of the client. Further, there is no teaching or suggestion of providing a signed common nonce and a client request from a middle tier server to at least one back-end server so as to authenticate the client to the back-end server for implementation of the client request on behalf of the client.

In view of the clarifying comments and remarks above, the applicants respectfully request that the rejection to claim 1, and the claims that depend therefrom, be withdrawn.

Claims 26 and 27 recite analogous elements (in system and computer program product form) to that described above with reference to claim 1. As such, the arguments set out above apply by analogy. In view of the above, the applicants respectfully request that the rejection of claims 26 and 27 be withdrawn.

With respect to claim 28, *Bartolomeos* in view of *Kaliski* fails to teach or suggest at least:

> A method of authenticating a client, comprising…
> …receiving a pre-nonce token and a common nonce that has been signed by a client at a back-end server of a plurality of back-end servers from a middle tier server that is impersonating the client…

As noted in greater detail above, *Bartolomeos* and *Kaliski,* alone or in combination, fail to teach or suggest a common nonce that has been signed by a client at a back-end server of a plurality of back-end servers from a middle tier server that is impersonating the client as set out more fully herein.

Still further, *Bartolomeos* and *Kaliski* even when combined fail to teach or suggest:

> the common nonce is created by hashing the pre-nonce token and is generated from an entity other than the client that the middle tier server is impersonating or the plurality of back-end servers that the middle tier server is to interact with on behalf of the client…

As noted in greater detail herein, *Bartolomeos* fails to teach or suggest a nonce at all. In *Kaliski,* there is no teaching or suggestion that the client first hashes the message that it signs. Moreover, as noted in greater detail herein, *Kaliski* discloses that it is the client that creates the message, which fails to teach or suggest that the common nonce is generated from an entity other than the client that the middle tier server is impersonating or the plurality of back-end servers that the middle tier server is to interact with on behalf of the client.

Still further, *Bartolomeos* and *Kaliski* even when combined fail to teach or suggest:

> authenticating the client based on the received signed common nonce…hashing the pre-nonce token using the same hashing technique used to create the common nonce from the pre-nonce token … verifying the middle tier server based upon a comparison of the received common nonce and hashed value of the received pre-nonce token.

There is no teaching or suggestion anywhere in *Bartolomeos* that a back-end server authenticates both a client and a middle-tier server. Analogously, *Kaliski* is also silent with regard to a teaching or suggestion of hashing the pre-nonce token using the same hashing technique used to create the common nonce from the pre-nonce token … verifying the middle tier server based upon a comparison of the received common nonce and hashed value of the received pre-nonce token, which is recited in claim 28 *as amended herein.* Even when combined, the teaching is completely missing.

In view of the clarifying remarks and comments herein, the applicants respectfully request that the rejection of claim 28 be withdrawn.

Claims 29 and 32 recite analogous elements (in system and computer program product form) to that described above with reference to claim 28. As such, the arguments set out above apply by analogy. In view of the above, the applicants respectfully request that the rejection of claims 29 and 32 be withdrawn and the claims that depend therefrom be withdrawn.

Claims 4, 6, 12, 13 and 20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over *Bartolomeos* in view of *Kaliski* in further view of Schneier – Applied Cryptography (hereinafter, '*Schneier*').

The applicants respectfully assert that the above claims are patentable over the cited art at least by virtue of being dependent upon a base claim that the applicants assert is patentable as set out more fully above. In view of the clarifying remarks herein, the applicants respectfully request that the above rejections are withdrawn.

Claims 16-19, 21 and 22 stand rejected under 35 U.S.C. §103(a) as being unpatentable over *Bartolomeos* in view of *Kaliski* in further view of Menezes et al. (Handbook of Applied Cryptography). (hereinafter, '*Menezes*').

The applicants respectfully assert that the above claims are patentable over the cited art at least by virtue of being dependent upon a base claim that the applicants assert is patentable as set out more fully above. In view of the clarifying remarks herein, the applicants respectfully request that the above rejections are withdrawn.

Claim 23 stands rejected under 35 U.S.C. §103(a) as being unpatentable over *Bartolomeos* in view of *Kaliski* in further view of U.S. Pat. No. 6,054,784 to Day, (hereinafter, '*Day*').

The applicants respectfully assert that the above claim is patentable over the cited art at least by virtue of being dependent upon a base claim that the applicants assert is

patentable as set out more fully above. In view of the clarifying remarks herein, the applicants respectfully request that the above rejections are withdrawn.

Claims 24 and 25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over *Bartolomeos* in view of *Kaliski* in further view of *Menezes* and further in view of *Day*.

The applicants respectfully assert that the above claims are patentable over the cited art at least by virtue of being dependent upon a base claim that the applicants assert is patentable as set out more fully above. In view of the clarifying remarks herein, the applicants respectfully request that the above rejections are withdrawn.

New Claim

New claim 33 is believed to be patentable at least by virtue of being dependent upon a base claim that the applicants also believe is patentable as set out in greater detail herein. Moreover, the arguments described with reference to claim 28 apply by analogy to the new claim 33.

Conclusion

For all of the above reasons, the applicants respectfully submit that the above claims recite allowable subject matter. The Examiner is encouraged to contact the undersigned to resolve efficiently any formal matters or to discuss any aspects of the application or of this response. Otherwise, early notification of allowable subject matter is respectfully solicited.

Respectfully submitted,
Stevens & Showalter, L.L.P.
By
/Thomas E. Lees/
Thomas E. Lees Reg. No. 46,867

7019 Corporate Way
Dayton, Ohio 45459-4238
Phone 937-438-6848
Fax 937-438-2124